

ATTACHMENT B

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION**

UNITED STATES OF AMERICA

v.

OKELLO T. CHATRIE,

Defendant.

Case No. 3:19-cr-00130-MHL

DECLARATION OF SARAH RODRIGUEZ

I, Sarah Rodriguez, respectfully submit this declaration in regard to the above-captioned matter. I make this declaration based on my knowledge of the facts stated herein.

1. I am a Team Lead for Legal Investigations Support (LIS) at Google, where my responsibilities include processing law enforcement legal process requests directed at Google, including requests for Location History (LH) information. I joined Google in 2011 and have been in my current role since March 2018.

2. In my position, I am responsible for managing a team of LIS specialists who process and respond to certain law enforcement requests for data, including the LIS specialists involved in processing the search warrant in this case. I also process and respond to these requests.

I. Google's Production of LH Information to Law Enforcement In Response To Geofence Warrants

3. Google often receives search warrants from law enforcement authorities in the United States for a specifically identified Google user's Location History ("LH") information from a specifically identified time range. When producing data in response to such a demand,

Google searches for and retrieves only the responsive data that is associated with the particular users or accounts identified in the warrant.

4. Google also often receives search warrants from law enforcement in the United States for so-called “geofence” requests. Typically, such requests do not specify any known person, user, or account. Instead, geofence requests seek LH information for all Google users whose LH information indicates that their devices may have been present in a specified geographic area surrounding a point of interest, which law enforcement often indicates is a suspected crime scene, and a certain window of time, which might span a few minutes or a few hours.

5. Early “geofence” legal requests sought LH data that would identify all Google users who were in a geographical area in a given time frame. To ensure privacy protections for Google users and to protect against overbroad disclosures based on non-contextualized LH information, Google instituted a policy of objecting to any warrant that failed to include deidentification and narrowing measures. That protocol typically, as included in the search warrants, entails a three-step process.

6. First, law enforcement generally obtains a search warrant compelling Google to disclose a deidentified list of all Google user accounts for which there is saved LH information in a defined geographic area during a defined timeframe.

7. To comply with this first step of the process, Google must conduct the search across *all* LH data to identify users with LH data during the relevant timeframe, and run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant. Google does not know which users may have such saved LH data before conducting the search and running the computations.

8. After that search is completed, LIS assembles the stored LH records responsive to the request without any account-identifying information. This deidentified “production version” of the data includes a device number, the latitude/longitude coordinates and timestamp of the stored LH information, the map’s display radius, and the source of the stored LH information (that is, whether the location was generated via Wi-Fi, GPS, or a cell tower). The volume of data produced at this stage depends on the size and nature of the geographic area and length of time covered by the geofence request, which vary considerably from one request to another. LH records are deemed responsive to a geofence warrant (*i.e.*, a user’s estimated location is treated as falling within the scope of the warrant) if the stored latitude/longitude coordinates fall within the radius described in the warrant. That is true even if the shaded blue radius around those coordinates, which I understand reflects a 68% confidence interval around the location estimate, falls in part outside of the radius described in the warrant.

9. LIS deidentifies the data produced to the government at this step by removing the Google Account ID (an internal identification number assigned to the Google account that is associated to the device that is specific to each Google account) associated with the data, leaving only a device number that is used only in the Location History database. This device number is only used for distinguishing devices reporting LH to a user’s account, is not a valid account identifier (as it is not unique across accounts), and cannot be mapped to an Android ID, mobile equipment identifier (MEID), or international mobile station equipment identity (IMEI) number (as it is not unique across devices).¹

¹ An Android ID is an internal identification number assigned to each Android device connected to the Google Services Framework. *See* Google Pixel Phone Help, *Learn about the Android Device Configuration Service*, <https://support.google.com/pixelphone/answer/9021432?hl=en> (visited Feb. 28, 2020).

10. Second, the government reviews the deidentified production version to determine the device numbers of interest. If additional deidentified location information for a device in the production is necessary to eliminate false positives or otherwise determine whether that device is actually relevant to the investigation, law enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request (if authorized in that request).

11. This additional contextual LH information can assist law enforcement in eliminating devices in the production that were not in the target location for enough time to be of interest, were moving through the target location in a manner inconsistent with other evidence, or otherwise are not relevant to the investigation.

12. Finally, based on the deidentified data produced, the government can compel Google (if authorized in the request) to provide account-identifying information for the device numbers in the production that the government determines are relevant to the investigation. In response, Google provides account subscriber information such as the email address associated with the account and the name entered by the user on the account.

II. This Geofence Warrant

13. In this case, Google received a geofence warrant (Google Reference No. 2590472) dated June 14, 2019, that was submitted to Google's online system through Detective Joshua Hylton's verified account on June 20, 2019. The geofence warrant requested information about Google accounts associated with devices that reported a location located within a 150-meter radius around a specified latitude and longitude coordinate (described as an area surrounding a Federal Credit Union and located in Richmond, Virginia) between 4:20 P.M. and

5:20 P.M. on Monday, March 20, 2019. The warrant set forth the three-step process (described above), which Google followed.

14. A LIS specialist executed the query for searching across all LH data to identify users with LH data during the specified timeframe and to run the computations against every set of coordinates in order to determine which LH records matched the geographic parameters in the warrant. The LIS specialist then produced the deidentified “production version” of the LH records responsive to the request (*i.e.*, no account-identifying information) through Google’s online system to Detective Hylton’s online account on or about June 28, 2019. As described above, this production included the latitude/longitude coordinates and timestamp of the responsive stored LH information, along with a display radius around those coordinates (expressed as a distance in meters) that reflects Google’s confidence in the LH coordinates. A value of 100 meters, for example, I understand reflects Google’s estimation that the user was likely located within a 100-meter radius of the saved coordinates based on a goal to generate a location radius that accurately captures roughly 68% of users. I understand that the same calculation would apply to any other display radius given in the production.

15. On or about July 2, 2019, Google received an email from Detective Hylton requesting additional location data (*i.e.*, step 2) and subscriber information (*i.e.*, step 3) for all 19 device numbers produced in step 1.

16. On or about July 8, 2019, Google received two voicemails from Detective Hylton. A LIS specialist called Detective Hylton that day and explained the issues in the Detective’s email as the request did not appear to follow the three sequential steps or the narrowing required by the search warrant. Detective Hylton asked, and the LIS specialist explained, what information would be produced in step 2 and after in step 3. The LIS specialist also explained the importance of step 2 in narrowing. Detective Hylton stated that Google could run step 2 on

the first 9 device numbers in his email, dated July 2, 2019. Detective Hylton also stated that he would attempt to narrow further for step 3.

17. On or about July 9, 2019, Google received an email from Detective Hylton requesting additional location data (*i.e.*, step 2) on 9 device numbers.

18. A LIS specialist executed the query to search for the additional contextual location coordinates for the 9 device numbers beyond the time and geographic scope of the original request (as authorized in the search warrant). The LIS specialist then produced the deidentified "production version" of the LH records responsive to the request (*i.e.*, no account-identifying information) through Google's online system to Detective Hylton's online account on or about July 9, 2019.

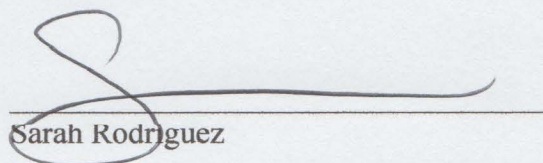
19. On or about July 10, 2019, and July 11, 2019, Google received emails from Detective Hylton requesting subscriber information (*i.e.*, step 3) on 3 device numbers.

20. A LIS specialist produced the account subscriber information associated with the 3 device numbers on or about July 11, 2019.

21. On or about July 12, 2019, Google received an email from Detective Hylton requesting additional device or phone number information that could be associated with one of the accounts that LIS produced subscriber information on in step 3. A LIS specialist called Detective Hylton on or about July 12, 2019, and no further information was produced under this search warrant.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 11th day of March 2020, in San Francisco, CA.



Sarah Rodriguez